Inside Security IT Consulting GmbH
Technologiezentrum
Nobelstr. 15
D-70569 Stuttgart

Tel: 0711-68 68 70 30
Fax: 0711-68 68 70 31
E-Mail: info@inside-security.de
Internet: www.inside-security.de

Allgemeine Vorgehensweise bei der Durchführung von Audits zur Überprüfung der Sicherheit von Computernetzwerken

Angelehnt an die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlene Systematik gehen wir bei der Durchführung von Sicherheitstests in fünf Schritten vor:

1. **Vorbereitungsphase** zur Vereinbarung von Art, Umfang und Zielsetzung der Tests mit dem Kunden

2. **Informationsbeschaffungsphase**, in der möglichst viele öffentlich zugängliche Informationen über das zu testende System beschafft werden

3. **Bewertung** der gewonnenen Informationen bezüglich Schwachstellen, die für Angriffe ausgenutzt werden können

4. **Angriffe** und damit der Versuch auf nicht öffentliche Informationen zuzugreifen

5. **Dokumentation** der durchgeführten Arbeiten, Erstellen eines Ergebnisberichts mit allen erkannten Schwachstellen und Verbesserungsvorschlägen

Ziel eines von uns durchgeführten Sicherheitsaudits ist die Verbesserung der technischen, organisatorischen und personellen Sicherheit des überprüften IT-Systems.

Bei der Durchführung unterscheiden wir zunächst nach Black Box Tests, bei denen wir vorab keine Details über das zu überprüfende System erfahren und White Box Tests, bei denen wir vom Kunden vor Testbeginn technische Einzelheiten des Systems erhalten. Ein Black Box Test simuliert daher eher die Situation eines tatsächlichen Angreifers, während ein White Box Test ein gezielteres und damit effizienteres Vorgehen ermöglicht.

Weiterhin unterscheiden wir zwischen externen Tests, die die Situation eines Angreifers über das Internet abbilden und internen Tests, mit denen wir die Angriffsmöglichkeiten von Personen mit physikalischem Zugang zum Intranet überprüfen.

Eine umfassende Sicherheitsüberprüfung besteht dabei aus den beiden Komponenten Penetrationstest und Sicherheitsaudit, wie im Folgenden beschrieben:

Penetrationstest:

In der Vorbereitungsphase wird mit dem Auftraggeber vereinbart, welche Systeme Ziel des Angriffs sein sollen, und welche davon ausgenommen werden. Ebenso werden Art und Agressivität der Angriffsversuche festgelegt; so werden zum Beispiel oft Denial of Service Angriffe ausgeschlossen.

Zur Vorbereitung eines automatisierten Portscans ermitteln wir dann zunächst manuell Antwortverhalten und Laufzeiten von IP-Paketen an erreichbare Rechner. Aus diesen Daten werden dann Parameter (z.B. Timeoutzeiten) für den automatisierten Portscan berechnet, um diesen mit zuverlässigen Ergebnissen durchführen zu können.

Der automatisierte Portscan der IP-Adressen liefert die erreichbaren Netzwerkdienste der Zielrechner, sowie über TCP/IP-Fingerprinting deren Betriebssystem. Von den Netzwerkdiensten wird anschließend in einem gezielten Versionsscan die verwendete Softwareversion ermittelt.

Mit Hilfe von Security Scannern werden die ermittelten Angriffspunkte auf Sicherheitslücken hin analysiert. Zusätzlich werden die ermittelten Versionen der verwendeten Software mit Hilfe einer Datenbank auf bekannte Verwundbarkeiten hin überprüft. Die Ergebnisse der Security-Scanner werden nochmals manuell überprüft, um falsche Positiv- und Negativergebnisse zu eliminieren.

Über die ermittelten Schwachstellen führen wir dann gezielt Einbruchsversuche durch. Dabei kommen sowohl Standardmethoden, die im Internet als fertige Angriffsprogramme angeboten werden, als auch eigenentwickelte Methoden und Angriffsprogramme zum Einsatz.

Sicherheitsaudit:

Hierbei führen wir eine grundlegende Analyse des Netzwerks durch, mit dem Ziel, Schwachstellen, die zu einer Kompromittierung des Intranets führen können, zu erkennen. Die verantwortlichen Administratoren können auf Wunsch jeden Schritt mitverfolgen und so aktiv ihr Wissen im Bereich IT-Sicherheit erweitern. Im Einzelnen werden folgende Arbeiten durchgeführt:

- Ist-Analyse des Netzwerks und Erstellen eines aktuellen Netzplans
- Bewertung der Netzwerkarchitektur unter Sicherheitsaspekten
- Analyse der physikalischen Absicherung der Netzwerkkomponenten
- Identifizierung von Schwachstellen und möglichen Einbruchspunkten
- Bewertung von Organisation und Management der Netzwerksicherheit

Das als Social Engineering bekannte Aushorchen und Bedrängen von Mitarbeitern mit dem Ziel interne Informationen zu erhalten, führen wir nur auf speziellen Wunsch des Auftraggebers durch. Unter der Voraussetzung, dass genügend Zeit und Agressivität eingesetzt wird, führt Social Engineering immer zum Ziel. Wir betrachten diese Art Test daher als teure Show mit bekanntem Ausgang und verzichten daher in der Regel darauf.